Amendments to the CLAIMS

This listing of the claims replaces all prior versions and listings of the claims in this application:

1. (Previously Presented) A method for distributing data over a network comprising:

issuing a certificate and a private key to a client for identifying the client in a transaction;

storing the certificate and the private key in a portable token of the client and used by the client during a transaction, the portable token being a physical device removeably coupleable to a client computer;verifying a digital signature using the certificate stored in the token before distributing data to the client;

generating a message associated with the data being downloaded to the client and associated with at least part of a distinguishing number for the token used by the client during a transaction; and

distributing the data and the associated message to the client.

2. (Original) The method of claim 1, further comprising providing the client with information necessary for establishing an account.

3. (Original) The method of claim 2, further comprising providing the client with the token.

4. (Currently amended) A method for distributing data over a network comprising:

establishing a secure connection between a client and a server;

issuing a certificate and a private key to the client for identifying the client in a transaction;

storing the certificate and the private key in a portable token of the client and used by the client during a transaction, the portable token including a unique distinguishing number and being a physical device removeably coupleable to a client computer; and

generating a message associated with the data being distributed to the client and associated with at least in part with the [[of a]] distinguishing number for the token used by the client during a transaction.

5. (Original) The method of claim 4, further comprising distributing data to the client.

6. (Original) The method of claim 5, further comprising requesting information from the client for establishing an account.

7. (Original) The method of claim 4, wherein establishing a secure connection comprises establishing a secure connection using a security protocol.

8. (Original) The method of claim 7, wherein the security protocol is the secure socket layer protocol.

9. (Original) The method of claim 6, wherein requesting information comprises requesting a credit card number.

10. (Original) The method of claim 6, wherein requesting information comprises requesting a password.

11. (Original) The method of claim 4, wherein storing the certificate comprises:
interfacing the token to a client computer; and
writing the certificate and the private key to the token across the network.

12. (Original) The method of claim 4, wherein storing the certificate comprises:
interfacing the token to a server computer; and
writing the certificate to the token at the server computer.

13. (Original) The method of claim 5, wherein distributing data to the client comprises distributing a media player.

14. (Currently amended) A method for distributing data over a network comprising:

establishing a secure connection between a client and a server;

receiving a request from the client for data to be downloaded;

generating a message associated with the data being downloaded to the client and associated with at least part of a distinguishing number for a portable token of the client and used by the client, the portable token being a physical device removeably coupleable to a client computer, the step of message generating comprising:

including in the message a data identification number,

including in the message a period of time for which the data may be used by the client, and

including in the message a symmetrical key used to encrypt the data when distributing data from the server to the client over the network;

and

distributing the data and the associated message to the client.

15. (Original) The method of claim 14, wherein establishing a secure connection comprises establishing a secure connection using a security protocol.

16. (Original) The method of claim 15, wherein the security protocol is the secure socket layer protocol.

17. (Original) The method of claim 14, wherein establishing a secure connection comprises

requesting authentication information from the client; and

sending authentication information from the server.

18. (Original) The method of claim 17,wherein requesting authentication information from the client comprises

requesting a certificate from the client; and

requesting a digital signature from the client.

19. (Original) The method of claim 17, wherein sending authentication information from the server comprises:

sending a certificate from the server; and

sending a digital signature from the server.

20. (Original) The method of claim 18, wherein requesting a certificate comprises reading the certificate from the token used by the client.

21. (Cancelled)

22. (Original) The method of claim 14, wherein generating a message further comprises generating a message using a public key (asymmetric) cryptographic algorithm.

23. (Previously presented) A method of securely utilizing downloaded data comprising:

opening a media player;

opening a data file;

requesting a portable token from and used by a client, the portable token being a physical device removeably coupleable to a client computer;

reading a distinguishing number from the token;

verifying a digital message associated with the data file and the token using the media player, the distinguishing number, and a private key in the token.

24. (Original) The method of claim 23, wherein in verifying a digital message, the media player reads the private key from the token to decrypt the digital message.

25. (Original) The method of claim 23, wherein in verifying a digital message, the media player sends the digital message to the token.

26. (Original) The method of claim 25, wherein the token decrypts an encrypted symmetric key using the private key.

27. (Previously presented) The method of claim 23, wherein verifying a digital signature comprises

verifying the distinguishing number read from the token;

verifying a time period associated with the data file;

decrypting an encrypted symmetrical key using the private key from the token;

decrypting the data file using the symmetrical key.

28-32. (Cancelled)